F9 Biometric Access Control Terminal

User Manual

Version 1.1
Date: July 2011

ZKSoftware®
Advanced Biometric and RFID Solutions

All design and specification declared are subject to change without notice in advance Copyright © 2009 ZKSoftware Inc. All rights reserved

Table of contents

1 Instructions 3

1.1 Fingerprint placement. 3
1.2 Instruction for card swipe 3
1.3 Precautions 3

2 Introduction of device 4

2.1 Overview of device functions 4
2.2 Product Appearance 4
2.3 Keypad 5
2.4 Date & Time 6
2.5 Voice Control 6
2.5.1 Turn On/Off 6
2.5.2 Adjust Volume 6
2.6 Security Features 6
2.6.1 Admin Affirm 6
2.6.2 Tamper Switch 6
2.7 Cleaning Terminal 6
2.8 Restarting & Restting the unit 7
2.8.1 Restarting terminal 7
2.8.2 Resetting terminal 7

3 Connections 7

3.1 USB Port 7
3.2 TCP/IP 7
3.2.1 Using TCP/IP 7
3.3 RS232/RS485/Wiegand port 8
3.3.1 Using RS232. 8
3.3.2 Using RS485. 8
3.4 Power supply port 8
3.5 Access control port 8
3.6 Using USB 8
3.6.1 Using USB 8
3.7 Communication Key 8

4 User 9

4.1 Enrolling user. 9
4.1.1 Fingerprint Enrolment 9
4.1.2 Card Enrolment 9
4.1.3 Password Enrolment 9

ZKSoftware®
The Advanced Biometric Solution

Table of contents...continue 1

4 User...continue 9

4.1.4 Fingerprint and password enrolment 9

4.2 Verifying user 10

4.2.1 1:1(one to one) / 1:N(one to many) 10

4.2.2 Voice message 10

4.2.3 Fingerprint verification 10

4.2.4 Password vrification 10

4.2.5 Card verification 10

4.3 Types of verification modes 11

4.4 Adding user information 11

4.5 Deleting user. 11

4.6 Access level/priviledge 11

5 System 11

5.1 General settings 11

5.1.1 Adjusting Date/Time 11

5.1.2 Date format 12

5.1.3 Voice 12

5.1.4 Volume % 12

5.1.5 User interface style 12

5.2 Fingerprint settings 12

5.2.1 Setting threshold 12

5.2.2 Auto alarm 12

5.2.3 Show score. 12

5.2.4 Defining work codes 13

5.3 System information 13

5.3.1 Number of users in the terminal 13

5.3.2 Quantity of templates stored 13

5.3.3 Quantity of attendance logs saved 13

5.3.4 Number of admins registered 13

5.3.5 Number of password user available 14

5.3.6 Number of time scanners used 14

5.3.7 Free space 14

5.3.8 Device information 14

5.4 Log information 15

5.4.1 Alarm super log 15

5.4.2 Alarm attendance log 15

5.4.3 Recheck min 15

ZKSoftware® The Advanced Biometric Solution

Table of contents...continue 2

6 Data 15
- 6.1.1 Deleteing transaction logs 15
- 6.1.2 Deleteing all data 15
- 6.1.3 Managing user priviledges 15
- 6.1.4 Resetting to factory settings. 15

7 USB 16
- 7.1 Understanding the need for USB 16
- 7.2 Type of USB 16
- 7.3 Downloading attendance logs 16
- 7.4 Downloading user data 16
- 7.5 Uploading user data from USB 16
- 7.6 Uploading short messages 16

8 Access 17
- 8.1 Using the terminal as door access. 17
- 8.2 Access options 17
  - 8.2.1 Time zone 17
  - 8.2.2 Grouping 17
- 8.3 User account options 18
- 8.4 Access combination 18
- 8.5 Lock 18
- 8.6 Door sensor delay 18
- 8.7 Door sensor mode 19
- 8.8 Door sensor alarm 19
- 8.9 Turning off alarm 19
- 8.10 Duress options 19
  - 8.10.1 Management of duress fingerprint 19
  - 8.10.2 Help key 19
  - 8.10.3 Trigger methods 20
  - 8.10.4 Alarm delay 20
- 8.11 Alarm count 20
- 8.12 Group verification type. 20

9 RFID card function 20
- 9.1 Understanding the RFID card 20
- 9.2 Enrolment of RFID card 20
- 9.3 Verification using RFID card only 20
- 9.4 Multi-verification methods 21
- 9.5 Deleting RFID card 21

ZKSoftware®
The Advanced Biometric Solution

Table of contents...continue 3

10 Autotest 21

10.1 Who should do the autotest 21
10.2 Run all tests at once 21
10.3 Flash test 21
10.4 LCD test 21
10.5 Voice test 21
10.6 FP reader. 21
10.7 Key test 22
10.8 RTC test 22

11 Troubleshooting 22

11.1 “Unable to connect” appears. 22
11.2 “Admin affirm” appears 22
11.3 Difficult to read finger 22
11.4 LED is blinking all the time 22
11.5 “Duplicate finger” appears 22
11.6 RFID card doesn’t respond 23
11.7 No sound. 23

12 System Specifications 23

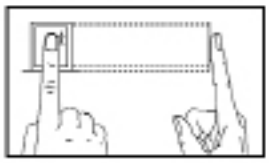
ZKSoftware®
The Advanced Biometric Solution

1. Intructions

1.1 Fingerprint placement

Recommended fingers: The index finger, middle finger or the ring finger; the thumb and little finger are not recommended (because they are usually clumsy on the fingerprint collection screen).

1. Proper finger placement:

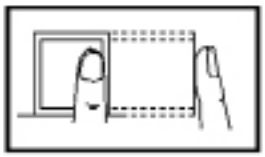


The finger is flat to the surface and centered in fingered guide.

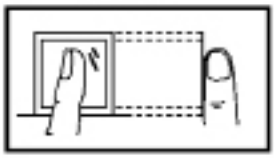
2. Improper finger placement:

Not flat to the surface

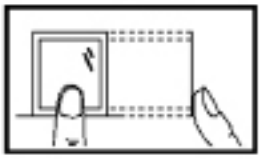
Off-center



Slanting



Off-center



Please enrol and verify your fingerprint by using the proper finger placement mode. We shall not be held accountable for any consequences arising out of the degradation in verification performance due to improper user operations. We shall reserve the right of final interpretation and revision of this document.

1.2 Instruction for Card Swipe

This device is supplied with an integrated non-contact RFID (125 MHz) card reader module. By offering multiple verification modes such as fingerprint, RF card, pin, RF card + fingerprint, fingerprint + RF card verification + pin. This device can accommodate diversified user needs.

Swipe your card across the sensor area after the voice prompt and remove your card after the device has sensed it. For the swipe area, see 2.2 Product Appearance.

1.3 Precautions

Protect the device from exposure to direct sunlight or bright light, this greatly affects the fingerprint collection and leads to fingerprint verification failure.

It is recommended to use the device under a temperature of 0–50°C so as to achieve the optimal performance. In the event of exposure of the device to the outdoors for long periods of time, it is recommended to adopt sunshade and heat dissipation facilities because excessively high or low temperature may slow down the device operation and result in high false rejection rate (FRR).

When installing the device, please connect the power cable after connecting other cables. If the device does not operate properly, be sure to shut down the power supply before performing necessary inspections. Note that any live-line working may cause damage to the device and the device damage arising out of live-line working falls beyond the scope of our normal warranty.

For matters that are not covered in this document, please refer to related materials including the installation guide, access control software user manual.

Summary

* Please ensure correct placement of finger on reader.

* 125 MHz RFID Cards can be used.

* Do not install in direct sunlight or bright light

* 0–50°C for optimal performance

* Shut down the unit and power before attempting maintenance

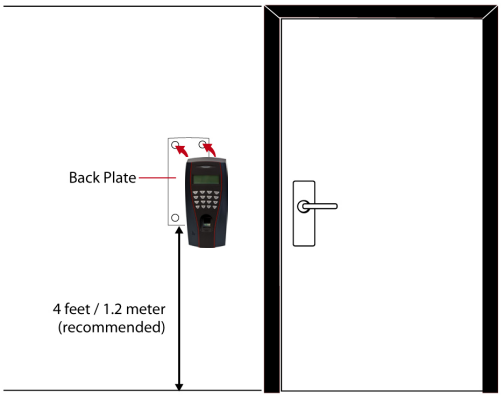
ZKSoftware®
The Advanced Biometric Solution

2. Introduction of Device

2.1 Overview of Device Functions

As an integrated fingerprint & access control device, our product can be connected with either an electronic lock or an access controller. This device features simple and flexible operations and supports the use of management cards. The screen displays will guide you through all the operations. It supports access control function for a security management. It supports multiple communication modes.

Attached the back plate on the wall securely and attach the terminal to the back plate when mounting it on the wall.



2.2 Product Appearance

Front view:

- **LCD Screen Displaying status of terminal, day, date and time.**
- **LED Display**
- **Green LED – The terminal is working fine and it is in standby mode.**
- **Red LED – There is an error at the terminal that requires checking. For first time use, the terminals need to be charged fully to avoid having the red light blinking.**
- **Keypad To input instructions into the terminal and to allow configuration.**
- **Fingerprint Sensor To scan finger for confirmation of identity.**
- **RFID Card scan Area Area that reads RFID cards.**
- **Speaker For terminal voice emission.**

Summary

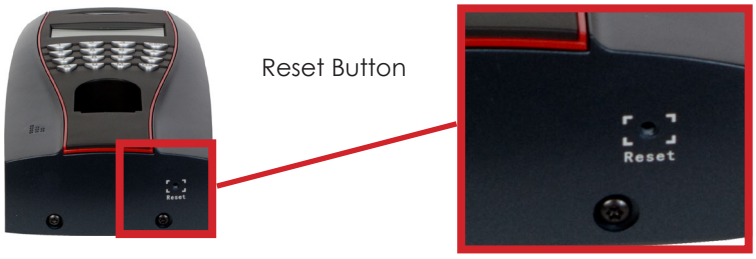
* Different user access modes availbale on the unit

* Install with backplate

* Recommended height from the floor - 1.2m

ZKSoftware®
The Advanced Biometric Solution

Bottom view:

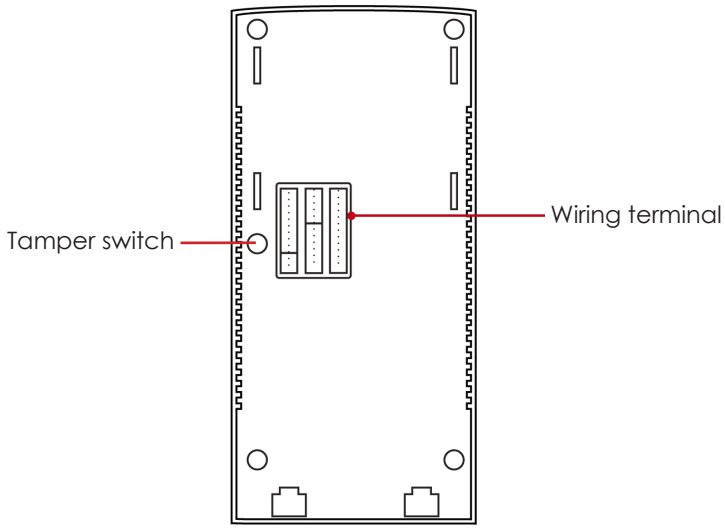


- **Reset button**: Used to restart the device.

Side View:

- **USB Port To upload/download users information, password and transaction logs via USB flash disk.**

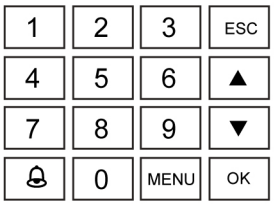
Rear View:



- **Wiring terminal**: Connects with locks and power supply through cables.
- **Tamper Switch**: Used to generate a tamper alarm.

2.3 Keypad

You can insert inputs into the terminals through the keypad. It contains numbers from 0-9, an OK button, an ESC/Cancel button, a Scroll up/down button, a doorbell button and a Menu button.



Summary

* Reset button is situated below the unit

* USB port is situated on the side of unit

* Keypad used for user password / pin entry and navigation of the unit

ZKSoftware®
The Advanced Biometric Solution

2.4 Date & Time

The terminals displays the date and time at the home screen. Choose the date and time format based on your preference.

Set your time and date:

- Press Menu > Options > Systems Options > Date/Time > set your time and save.

To change the date format:

- Press Menu > Options > Systems Options > Fmt > Determine the date format based on your preference.

2.5 Voice Control

Voice Control lets you control the level of volume emitted by the terminal.

2.5.1 Turn On/Off

The system lets you turn on/off the voice based on your preference.

- Press Menu > Options > System Option > Adv Option > Voice > Y/N.

2.5.2 Adjust Volume

The default volume of the terminal's voice is 67. The volume can go as high as 100 and as low as 0. To sustain the performance of the speaker, it's recommended to stay at range 60-70.

To adjust the volume

- Press Menu > Options > System Option > Adv Option > Adj VOL (%) > adjust accordingly .

2.6 Security Features

Security features help protect the information in the terminal from being accessed by unauthorized individuals.

2.6.1 Admin Affirm

Register an administrator into the system by enrolling fingerprints or a password to a user ID.

- Press Menu > User Manage > Enroll Admin > Choose enrollment method > Perform enrolment and Save.

After enrolling an administrator, the main menu can only be accessed by the administrator.

2.6.2 Tamper Switch

The fingerprint terminals come with a tamper switch located at the rear of the terminals. During installation, the tamper switch is compressed against the back plate. Any attempt to dismantle the terminal will trigger an alarm and a "System Broken" message will be displayed on the panel.

2.7 Cleaning Terminal

2.7.1 Cleaning The Body

Use a dry cloth to clean the terminal's body. Do not use any liquids, household cleaners, aerosol spray, solvents, alcohol, ammonia and abrasive solutions to clean the body of the terminal because it could damage it.

Summary

* Ensure correct time and date

* Ensure correct time and date format

* Toggle voice ON/OFF

* Adjust unit Volume

* Ensure to enrol administrator

* Tamper switch for added security on the unit

* DO NOT USE:

** Liquid

** Alcohol

** Ammonia

ZKSoftware®
The Advanced Biometric Solution

2.8 Restarting and Resetting Terminal

If a feature isn't functioning as it should, try restarting or resetting the terminals

2.8.1 Restarting the terminal

- Push the On/Off button or "reset button" on the terminal to restart the terminal. If you can't restart the terminal, or if the problem persists, you might want to reset.

2.8.2 Resetting the Terminal

- Press Menu > Option > System Option > Adv Opt > Reset terminal. Resetting of the terminal will cause all your settings to return to its original factory settings. Make sure that you have backed up all data before you proceed.

Summary

* If unit is not functioning as per normal, press the RESET button or the POWER button to restart the unit

* RESET will not delete any settings or data

3. Connections

3.1 USB Port

Linking with USB flash disk for remote data transfer.

* USB is used for data transfer

3.2 TCP/IP

Connect with CAT 5 cable for LAN connection, one end to this port and another end to the computer's TCP/IP Port.

TCP/IP for Single Connection – Linking the terminal to a single computer using TCP/IP requires Ethernet 10/100Base-T Crossover Cable. The cable can be used to cascade hubs or to connect Ethernet stations back-to-back without a hub. It works with both 10Base-T and 100Base-TX

* Unit can be connected to local LAN with CAT 5 cable

3.2.1 Using TCP/IP

Determining the IP Address

IP address is important, as it is a unique address of the terminal in LAN. Without the IP address, locating the specific terminal is not possible. To input the IP address of the terminal:

- Press Menu > Options > Comm Opt > IP Addr > Key in IP address.

* Insert an IP Address

* Unit does not opporate with DHCP

Setting up Ethernet

It is important to setup the Ethernet to connect the terminals using TCP/IP connection. Setting up Ethernet is by enabling the Ethernet function:

- Press Menu > Options > Comm Opt > Ethernet > Yes. Turn off the terminal after you have set the Ethernet to Yes. Now, plug the network plug to the Ethernet interface and turn the power on.

Determining the Netmask, Gateway and NetSpeed: For TCP/IP connection, please configure the netmask, gateway and netspeed for the terminal.

- Press Menu > Options > Comm Opt > NetMask > Insert the numbers.
- Press Menu > Options > Comm Opt > Gateway > Insert the numbers.
- Press Menu > Options > Comm Opt > NetSpeed > Choose the speed of your Ethernet connection

ZKSoftware®
The Advanced Biometric Solution

3.3 RS232/RS485/Wiegand port

- **RS232** – Connection to a computer using RS232 cable.
- **RS485 Single Connection** - Connection to a single computer using RS485 wire.
- **RS485 Network Connection** - Connection to multiple computers using Daisy Chain connection.
- **Wiegand Output** – Connecting with third party connector or terminal(s).

3.3.1 Using RS232

For connection via RS232, baudrate is the determinant of communication speed between the terminal and the software. The higher the baudrate, the faster the speed is.

To turn on RS232 connection and set the baudrate:

- Press Menu > Options > Comm Opt > RS232 >

Change the RS232 connection to Y. To change baudrate:

- Press Menu > Options > Comm Opt > Baudrate > Change the Baudrate accordingly.

3.3.2 Using RS485

For connection via RS485, baudrate is also the determinant of communication speed between the terminal and the software but the speed must be according to the speed of the converter. Check your converter for the speed.

To turn on RS485 connection and set the baudrate:

- Press Menu > Options > Comm Opt > RS232 > Change the RS485 connection to Y .

To change baudrate:

- Press Menu > Options > Comm Opt > Baudrate > Change the Baudrate accordingly.

3.4 Power supply port

Insert the Power Adapter point to this port for power. (DC12v)

3.5 Access control port

Linking the terminal to door lock system.

3.6 Using USB

USB flash disk is useful in cases where the terminal is installed far from a PC or there is a connection problem.

3.6.1 Using USB

- Press Menu > PenDrive Mgmt > Choose the operation that you want to carry via USB

3.7 Communication key

Since the software is controlled by an activation code and product key, set the COMM key to zero.

- Press Menu > Options > Comm Opt > COMM Key > 0

Summary

* Set BAUDRATE to use RS232 connection

* BAUDRATE must accomodate converter speed

* Set COMM KEY to “0”

ZKSoftware®
The Advanced Biometric Solution

4. User

4.1 Enrolling User

The terminals can enroll fingerprint templates, passwords and card information. This chapter covers all possible user enrollments in the terminals. Caution: Enrollment of supervisor or administrator is important to ensure the terminals data safety. Prior to enrolling a new user, a supervisor has to be enrolled first by using any of the methods mentioned below. Select Enroll Admin > Choose the Privilege Level either Supervisor or Administrator to proceed.

Summary

* Ensure to enrol an administrator on the unit before enrolling users

4.1.1 Fingerprint Enrolment

It is recommended to enroll two fingers for one user ID. One template is default and another one is used for backup. You need to check the quality of the fingerprint before doing any fingerprint enrollment. It is important to locate the center points of the finger because the center points has to be placed in the middle of the scanner during enrollment to get a good reading. Refer to page 19. You also have to make sure that the fingers are not too wet or too dry for enrollment.

* Recommend to enrol more than 1 finger per user

Enrolling fingerprint:

- Press Menu > User Manage > Enroll User > Enroll FP > New Enroll > OK > Place finger 3 times > (OK) Save > ESC to exit, New Enrol (Continue?) – OK to proceed to enroll another fingerprint.

Enrolling backup fingerprint:

- Press Menu > User Manage > Enroll User > Enroll FP > ESC > Input User ID > Place finger 3 times > (OK) Save > ESC to exit, New Enroll (Continue?) – OK to proceed to enroll another fingerprint.

4.1.2 Card Enrolment

The default card for the terminal is the RFID card. MiFare and HID card systems are available upon request.

* If problem exists with user fingerprint, issue a RF Card

Enrolling card:

- Press Menu > User Manage > Enroll User > Reg RFID > New Enroll? > OK > Key in User ID (PIN) > Wave the card at the scanning area until the screen displays the Card ID > (OK) Save

4.1.3 Password Enrolment

The terminals offer password verification and the maximum length of password is 5 digit. Enrolling password: Press Menu > User Manage > Enroll User > Enroll Pwd > New Enroll? > OK > Key in User ID (PIN) > OK > Input your password > LCD showing the ID with minus -P to indicate that the user ID is using password > OK (Save)

* Password / pin options available for added security

Changing password:

- Press Menu > User Manage > Enroll User > Enroll Pwd > ESC > Input User ID > OK > Change your password > LCD showing the ID with minus -P to indicate that the user ID is using password > OK (Save)

4.1.4 Fingerprint and Password Enrolment

The terminals offer a combination of fingerprint and password enrollment for better security.

Enrolling FP and password:

- Press Menu > User Manage > Enroll User > FP & Pwd > New Enroll? > OK > Key in User ID (PIN) > OK > Input your fingerprint > Input your password and confirm the password one more time > LCD is showing the ID with minus -OP to indicate that the user ID is using a combination of fingerprint and password > OK (Save) Linking with USB flash disk for remote data transfer.

ZKSoftware®
The Advanced Biometric Solution

4.2 Verifying user

4.2.1 1:1 (One to One) / 1:N (One to Many)

VERIFICATION METHOD WHAT IS IT FOR

- 1:1 (One to One) You have to identify your User ID before inputting any biometrics feature for verification. For example, your user ID is 1008. One to one method requires you to key in user ID followed by your fingerprint to get verified.
- 1:N (One to Many) You don't need to identify your User ID before inputting any biometrics feature for verification. Simply place your finger on the scanner for verification.

4.2.2 Voice Message 🗣

VOICE / MESSAGE WHAT DOES IT MEAN?

- 🗣 ***"Verified"*** - Identity verification is successful, the terminal stores the transaction logs and opens the door (if connected to door access)
- 🗣 ***"Try again please"*** - Identity verification is failed because the finger is not properly positioned, the template is not available in the terminal or the password is incorrect.
- 🗣 ***"Admin Affirm"*** - You are not an administrator of the system and you cannot access Menu page
- 🗣 ***"Duplicate Finger"*** - This message only appears during registration when the finger that you want to enroll has been enrolled before. "FP Enrolled Already" will be displayed on the LCD screen.
- 🗣 ***"Invalid ID"*** - For 1:1 verification, User ID entered does not match with fingerprint.

4.2.3 Fingerprint Verification

1:N – 1:N verification does not require any input of your user ID. Place your finger properly on the scanner and the terminal takes second to verify your identity

1:1 – 1:1 requires input of User ID before the terminal reads and verifies. Input ID on the screen > Press OK button > the terminal reads and verifies.

Precautions

Some precautions have to be taken to get a good read every time.

- Make sure the center point of your finger is placed in the middle of the scanner for a good read.
- Recommended to use index finger. The terminal accepts other fingers but index is the most convenient.
- Make sure the finger is not wet, too dry, injured or dirty
- Do not press hard on the sensor, just place it comfortably
- Avoid direct sunlight or bright light

4.2.4 Password Verification

Password is an option for those who prefer not to use other verification methods. To verify via password, insert User ID > OK > insert password and press OK.

4.2.5 Card Verification

Place the card on the card scanning area and the terminal will read and verify the card

Summary

* 1:1 - User need to enter his ID first before scanning fingerprint
* 1:N - No need to enter ID

* Correct placement
* Recommend index finger
* Finger must be dry and clean
* Don't press to hard
* Avoid bright light

ZKSoftware®
The Advanced Biometric Solution

4.3 Types of verification methods

The fingerprint terminals offer various verification methods which include fingerprint (FP), User ID (PIN), Password (PW), and RFID (RF). You can configure the terminal to offer multi verification methods.

- Press Menu > Options > Access Options > Group VerType > Select the Group > OK > Select the time > OK > Down arrow and select Verification Type > OK

The terminals support the following combinations of verification:

VERIFICATION TYPE	DESCRIPTION
FP	Fingerprint only
PIN	User ID only
PW	Password only
RF RFID	Card only
FP/PW	Fingerprint or password
FP/RF	Fingerprint or RFID Card
PW/RF	Password or RFID Card
PIN & FP	User ID & Fingerprint
FP & PW	Fingerprint & Password
FP & RF	Fingerprint & RFID Card
FP/ PW/ RF	Fingerprint or Password or RFID. One method only
FP & PW & RF	Fingerprint, password & RFID, all methods are required
PIN & FP & PW	User ID, fingerprint & password, all methods required
FP & RF / PIN	Fingerprint & RFID card or 1:1 fingerprint matching

4.4 Adding User Information

User information can be added into terminals through the software. After the information is updated, sync with the terminal to display the information.

4.5 Deleting User

Only an administrator can perform user deletion at the terminal. To delete certain user(s):

- Press Menu > User Manage > Delete > Input User ID > The terminal will tell you the verification method enrolled by the user ID > OK > Prompting you to Delete User > Press OK > Confirmation is required > OK as Yes and Esc as No

4.6 Access Level/Privilege

The terminal offers various types of access level or privilege.

5. System

5.1 General Settings

5.1.1 Adjusting Date/Time

The function of the terminal is to record time attendance and door access activities of employees. Precision in time and date cannot be compromised for the system to work efficiently. Adjust Date/Time according to your time zone.

- Press Menu > Options > System Opt > Date/Time > Select Value > OK

Summary

* Depending on security level, you can use more than one verification setup

* Only administrator can delete users

* Ensure correct date & time

ZKSoftware®
The Advanced Biometric Solution

5.1.2 Date Format

Date format differs based on countries for example in Malaysia the format used is, date month year whereas in America, month comes first. Choose your date format according to your preference. The default format is dd-mm-yy.

- Press Menu > Options > System Opt > Fmt > Select Format > OK

5.1.3 Voice

The terminal has certain voice commands to guide users during enrolment and to notify users during the identity verification process.

- Press Menu > Options > System Opt > Adv Option > Voice > Y/N

5.1.4 Volume (%)

Voice Control lets you control the level of volume emitted by the terminal.

Adjust Volume: Default volume of the terminal's voice is 65. The volume can go as high as 100 and as low as 0. To sustain the performance of speaker in the terminal it's recommended to stay at range 60-70. To adjust the volume

- Press Menu > Options > System Opt > Adv Option > Adj VOL (%) > Set your number > OK.

5.1.5 User Interface Style

The terminals offer different user interface style. Select your style based on your preference.

- Press Menu > Options > UI Style > Select your style > OK

5.2 Fingerprint Settings

Configure the settings for fingerprint enrolment and verification to achieve optimum effectiveness.

5.2.1 Setting Threshold

Threshold determines how many percent of minutiae points on a fingerprint template is being read by the system. The higher the threshold level, the more points are being read, and the more restricted the system.

For 1:1, the range is from 15-50 and the recommended value is 35.
For 1:N, the range is from 5-50 and the recommended value is 45.

1:N – Match Threshold:

- Press Menu > Options > System Opt > Adv Option > Match Threshold > Determine the Level > OK

1:1 – 1:1 Threshold:

- Press Menu > Options > System Opt > Adv Option > 1:1 Threshold > Determine the Level > OK

5.2.2 Auto Alarm

Auto Alarm allows you to connect the terminal to third party alarm system. Menu > Options > System Opt > Adv Option > Auto Alarm > Y/N > OK

5.2.3 Show Score

The algorithm reads the minutiae points on a fingerprint for verification. This operation allows you to choose to display the number of points being read. If you choose Y, the number will be displayed on the top right corner of the LCD screen. Menu > Options > System Opt > Adv Option > Show Score > Y/N > OK

Summary

* Ensure correct date & time format

* Voice control ON/OFF

* Higher threshol for added security

* Change threshold according to security restrictions

ZKSoftware®
The Advanced Biometric Solution

5.2.4 Defining Work Codes

The fingerprint terminal provides work code feature which allowing user to key in a predefined numbers after verification. The work code numbers are predefined in software. The following table is showing examples of work codes.

Reasons	Work code
Check In	00
Check Out	01
OT start	04
Done	05
Sick Leave	10
Half-day Leave	12
Emergency Leave	11
Meeting Client	20
Outstation	21

Workcode Mode 1: Verification followed by work code

Workcode Mode 2: Work code followed by verification

To disable: Select No

- Press Menu > Options > System Opt > Adv Option > Work Code > OK > Select Preference > OK

5.3 System information

The terminals keep information of the system and this information is available for viewing by administrators.

5.3.1 Number of Users in the Terminal (User Count)

Every model of the terminal has different user capacity depending on the number of templates a user has in a terminal. For example, if a terminal could contain 3000 fingerprint templates and a user is entitled to 2 templates enrolment, the total user of the system would be 1500. To find out how many users are enrolled in a terminal:

- Press Menu > Sys Info > User Cnt > View the number

5.3.2 Quantity of Fingerprint Templates Stored in the Terminal (FP Count)

(This feature is NOT available in TimeLine 100 model.) The terminals contain fingerprint templates and the capacity differs from one model to another. To find out the number of fingerprint count in the terminal:

- Press Menu > Sys Info > FP Cnt > View the number

5.3.3 Quantity of Attendance Logs Saved In the Terminal (Att Log)

Once verification is completed, an attendance log will be stored in the terminal as record. A terminal can contain up to 120,000 logs depending on the models.

- Press Menu > Sys Info > AttLogs Cnt > View the number

5.3.4 Number of Administrators Registered in the Terminal (Admin Count)

A company can enroll several administrators to manage the system. This function enable the company to check the number of administrator present for a particular terminal.

- Press Menu > Sys Info > Admin Cnt > View the number

Summary

* Customised work codes available

* Total user count must be devided by number of fingerprints per user

** 3000 / 2 (p/user) = R1500

* Attendance logs need to be monitored

ZKSoftware®
The Advanced Biometric Solution

5.3.5 Number of Password Users Available in the Terminal (Password User)

Users can do verification using PIN password and a combination of fingerprint and password. To find out how many users are using password:

- Press Menu > Sys Info > Password User > View the number

5.3.6 Number of Time Scanners Have Been Used for Verification (S Logs)

S logs stands for scanner logs, which means the number of times the scanner has been used for verification, regardless of whether it is successful or not. To view the scanner logs:

- Press Menu > Sys Info > S Logs > View the number of S Logs

5.3.7 Free Space Information (Free Space)

Find out the information about availability of space in your terminal through this function.

- Press Menu > Sys Info > Free Space > View the info Information available includes fingerprint count, att log and S logs.

5.3.8 Device Information (Dev Info)

Find out the information about your terminal through this function. Press Menu > Sys Info > Dev Info > View the info

Information available includes:

- **AttLog (10k)**: Shows the number of attendance logs that can be stored in the terminal, for example for AttLog (10k) 12 means 10,000 x 12 = 120,000
- **S Logs**: Shows the number of Scanner Logs available for the terminal.
- **Manufactured Time (Manu Time)**: The date and time when the terminal was produced is displayed when you press Manu Time
- **Serial Number of the Terminal (Serial Num)**: The serial number of the terminal is important to activate the software and to liaise with FingerTec Worldwide in support issues. The Serial number is pasted on the back of the terminal but in case the sticker is damaged, this is where you can retrieve the serial number.
- **Manufacturer:** Get the name of the manufacturer of the terminal here.
- **Device Name**: All models have different names. If you don't know the name of the terminal that you are having, get it here.
- **Algorithm Version**: FingerTec Worldwide has already released a few algorithm versions into the market since the year 2000. New algorithm version comes with some improvements. This is where you can find terminal's algorithm version.
- **Firmware Version**: Support sometimes require a firmware version to resolve some support issues. The version and date of the version is released is provided here. **For example**: Ver 6.20 Aug 19 2009
- **View MAC**: This feature is a security feature of the products. Linking Software to the terminal requires the correct MAC address. Without availability of MAC address, the software will not be activated correctly. All products are supplied with the correct MAC address to ease communication. This is also to hinder people from using the software with a different hardware brand. An example of a MAC address is 00:0A:5D F1 BE 57.
- Press Menu > Sys Info > Dev Info > View MAC
- **MCU Version**: An MCU is the Main Controller Unit for the terminals. Version of the MCU determines the features and functions the terminal carries. To check the MCU Version:
- Press Menu > Sys Info > Dev Info > MCU Version

Summary

* Check number of password / pin users

* Free space includes the total ATT LOGS, Fingerprint count and S LOGS

ZKSoftware®
The Advanced Biometric Solution

5.4 Log Information (Log Opt)

A terminal can only retain certain amount of information before the terminal becomes full and stops accepting anymore data . To maintain the performance of a terminal, you can set an alarm to alert you when the data reaches a certain warning level.

5.4.1 Alarm Super Log

To instruct terminal to alert user if the transaction storage for administrator login is less than as configured. Default value is 99.

5.4.2 Alarm Attendance Log

To instruct terminal to alert user if the transaction storage is less than as configured. Default value is 99

5.4.3 Recheck Min

To instruct terminal to update clocking times of all users in a time interval. Default is 10 mins.

6. Data

Every time an enrolment is performed or a verification is done, a transaction log is created and stored inside the terminal. The data contains created terminal ID, date, time, userID and transaction activity.

- For example, 0105021009000000000010000:

These logs need to be managed to maintain the effectiveness of the terminal. There are 5 functions available in Data icon to enable you to manage data in the terminals

6.1.1 Deleting Transaction Logs

Delete Attendance Logs: The fingerprint terminal stores every transaction logs of its user. Once a user is enrolled and verified, the logs will be kept in the terminal. Please be certain before performing this operation because once the OK button is pressed, all attendance logs will be lost.

- Press Menu > Options > System Opt > Adv Option > Del Attlogs > OK > Delete? OK

6.1.2 Deleting All Data

Clear All Data: The fingerprint terminal contains all user data including User ID, verification methods, fingerprint templates, logs, etc. This operation allows deletion of all data in the terminal. Please be certain before performing this operation because once the OK button is pressed, all data will be lost.

- Press Menu > Options > System Opt > Adv Option > Clear All Data > OK > Delete? OK

6.1.3 Managing User Privileges

Clear Admin Privilege: To access system menu, it is recommended to enrol administrator to the system. Once administrator is enrolled, every time someone presses the Menu button, Admin Affirm message will be displayed. Clear Admin Privilege operation allows the current administrator to clear all his/her data to make way for the new administrator's data. Once the operation is completed, system menu is accessible by all users.

- Press Menu > Options > System Opt > Adv Option > Clr Admin Pri > OK > Continue? > OK

6.1.4 Resetting to Factory Settings

Reset Option: This feature is to restore all settings in the terminal to return to the original factory settings. You have to be certain before conducting this operation because once the OK button is pressed the terminal will be reset automatically.

- Press Menu > Options > System Opt > Adv Option > Reset Opts > OK. Please redo all the settings to suit to your company's requirements.
- Press Menu > Data icon > Restore to Factory Settings > Confirmation is required (Yes/No)

Summary

* System will stop if buffers are full

* Ensure warning alarm values are set

* Ensure to delete transaction logs regulary

* Deleting all data includes
** user id
** verification methods
** fingerprints
** Logs

* Enure all necessary data is backed up before performing this function

ZKSoftware®
The Advanced Biometric Solution

7. USB

7.1 Understanding the Need for USB Flash Disk

Communication between the terminal and a PC is very important to upload and download transaction data for time attendance and door access reports. The terminal offers a few communication options such as LAN and serial cable connections but sometimes there are scenarios that require USB (Universal Serial Bus) connectivity. USB can connect to the terminal with a computer for download and upload of user information and transaction logs. In the terminal, the USB Flash Disk function is known as Pen Drive Management.

Summary

* If unit is used as a standalone, data can be managed via USB

7.2 Type of USB

There are various types of USB available in the market. The terminal can only work with USB flash disks that support minimum Linux Kernel 2.4.x, working fine with Imation, Transcend and Pen Drive (minimum support Linux Kernel 2.4.x)

* Linux Kernel 2.4.x

7.3 Downloading Attendance Logs

To download attendance logs from the terminal to the computer:

- Press Menu > Pen- Drive Mng > DwnLoad AttLog > The terminal would require you to plug in the USB Flash Disk to proceed. After the download process is complete, eject USB Flask Disk from the terminal and connect it to your PC that has been installed with the software. Upload the data from the USB into software for further processing.

7.4 Downloading User Data

Enrollment of user must be done at the terminal. During enrollment, user data such as name and user ID are entered. To sync the data between the terminal and computer:

- Press Menu > PenDrive Mng > DwnLoad User > The terminal would require you to plug in the USB Flash Disk to proceed.

7.5 Uploading User Data from USB to Terminal

While administrator can input user data from the terminal, the rest of the users information is completed in the software. Get the latest updates of user information from the software to the terminal by using a USB Flash Disk.

* Downloaded user data can be uploaded to other units

- Press Menu > PenDrive Mng > UpLoad User > The terminal would require you to plug in the USB Flash Disk to proceed.

7.6 Uploading Short Messages

Some the terminals can display a short messaging system on the LCD. The SMS can be private or public. To assign sms to an individual or all staff using USB:

* Short message will display when user clocks in

- Press Menu > PenDrive Mng > Upload SMS > Insert the USB Flash Disk to proceed

8. ACCESS

8.1 Using The Terminal as Door Access

The terminals can be connected to door access accessories like electromagnetic lock, door bolt, exit button, etc to control access to doors. Make sure you understand the access options offered in the terminal and do necessary configurations for your door access system.

* Units can be connected to access control systems

ZKSoftware®
The Advanced Biometric Solution

8.2 Access options

This function determines user's accessibility or authority to enter certain doors.

8.2.1 Time Zone

The period where a user is allowed access is called TIME ZONE or time period (TP). In total there are 50 time zones available in FingerTec fingerprint models. Each Time Zone has 7 time slots for Monday until Sunday. To define time zone:

- Press Menu > Options > Access Options > Define TP > Select the Time Zone number and determine the time for each day.

Example 1

TIME ZONE	SUN	MON	TUE	WED	THU	FRI	SAT
1	0900:1800	0900:1800	0900:1800	0900:1800	0900:1800	0900:1800	0900:1800

What does Time Zone 1 mean?

Time Zone 1 consists of a constant access time for a period of one week where a user checks in at 9:00 and leaves at 18:00

Example 2

TIME ZONE	SUN	MON	TUE	WED	THU	FRI	SAT
2	0000:2359	0800:1200	0800:1200	0800:1200	0800:1200	0800:1200	0000:2359

What does Time Zone 2 mean?

Time Zone 2 is showing variation in access schedule from 8am-12pm from Mondays to Fridays and users are not allowed any access on the weekends.

Example 1

TIME ZONE	SUN	MON	TUE	WED	THU	FRI	SAT
3	0000:2359	1400:1800	1400:1800	1400:1800	1400:1800	1400:1800	0000:2359

What does Time Zone 3 mean?

Time Zone 3 is showing variation in access schedule from 2pm-6pm from Mondays to Fridays and users are not allowed any access on the weekends

8.2.2 Grouping

When a group of users are having an almost similar time zone assignment, they can be grouped together. For example, Time Zone 2 and Time Zone 3 are suitable for one group where users in this group checks in at 8:00 until 12:00 has a, break time from 12:00 to 14:00 , continue from 14:00 to 18:00, and no one is allowed access during weekends. Therefore, these users will be in Group Time Zone 1. The table below illustrates the Group Time Zone concept.

GROUP TIME ZONE	TIME ZONE	TIME ZONE	TIME ZONE
1	2	3	

There are a total of 5 Group Time Zones available in the system. The system default is Group 1 and Time Zone 1. Therefore, the newly enrolled users automatically will be in an unlocking status. If those users are not included in the grouping combination setting, they are given permission to record attendance but they can't unlock any door. To define Group Time Zone:

- Press Menu > Options > Access Options > GRP TP Define >

There are a total of 5 Group Time Zone offered and each Group Time Zone accepts only 3 time zones.

Summary

* It's recommended to use software to configure time zones

* Time zones allow entry in alotted time frame

* Users can be be entered into groups that are defined into different time zones

ZKSoftware®
The Advanced Biometric Solution

8.3 User Account Options

Summary

After a user has been enrolled, you can configure his/her access option settings.

- Press Menu > Options > Access Options > User Acc Opts > Input the user ID that you want to set the access option for > Determine the below matter:

USER ACC OPTS	WHAT YOU SHOULD DO
Belong to Group	Select group for this user
Use Group TPs	Yes or No
TP1	Select your Time Zone number 1
TP2	Select your Time Zone number 2
TP3	Select your Time Zone number 3
VERType	Select the verification type. 15 available
Use Grp VS	Yes or No

8.4 Access Combination

Access Combination is when you combine different users' verification in order to gain access. The system offers 10 different Access Combos and each combination applies to 3 Group Time Zones:

ACCESS COMBO	GROUP TIME ZONE	
1	1	TP1: 0900 – 13:00
	2	TP2: 1000 – 1500
	3	TP3: 1300 - 1400

* Use combo sets for added security (2 or more users need to verify before access)

To use the Access Combo, users from all the three time zones must be present for verification and the time period of the three groups must be valid in order to gain access. As shown in these time zones, 13:00 is the overlapping time where all of them can gain access.

To configure Access Combo:

- Press Menu > Options > Access Options > Access Comb > Select the combination you want for example Comb1 > OK > input the number, in this case 123 to represent GRP TP1, GRP TP2, GRP TP3> OK

8.5 Lock

The opening period of the electromagnetic lock or door bolt can be controlled according to your requirement or preference. The default value is 150 which translates to 3 sec. 50 is equivalent to 1 second.

* Ensure to set maglock time settings

- Press Menu > Options > Access Options > Lock > Determine the value of lock delay.

8.6 Door Sensor Delay

Door sensor delay can be configured to alert users if a door is not closing well after a time period. A door sensor must be installed prior to activation of this option. The default period is 10seconds and the maximum period is 999seconds.

* Install door sensor prior to activating this option

- Press Menu > Options > Access Options >Dsen Delay > Determine the value of lock delay.

ZKSoftware®
The Advanced Biometric Solution

8.7 Door Sensor Mode

Door sensor mode is to configure the time to alert an internal buzzer if the door is not closing properly. The standard of door locking system includes:

- **Normally Closed (NC)**: An electrical contact that regularly allows electricity to flow until it is signaled to open
- **Normally Open (NO)**.: An electrical contact that rarely allows electricity to flow. To use door sensor, select NC. Press Menu > Options > Access Options > Dsen Mode > Determine the type correctly > OK

8.8 Door Sensor Alarm

Door Sensor Alarm can be configured to alert users by using the alarm system if a door is not closing well after a time period. An alarm system must be installed first to use this operation.

- Press Menu > Options > Access Options > Dsen Alarm > Determine the period > OK

8.9 Turning Off Alarm

There are scenarios that require you to turn off your alarm system and this can be done through the terminal. To do this you have to press and hold the security button at the back of the terminal followed by

- Pressing Menu > Turn Off Alarm .If you didn't press the security button, the message "System Broken!!!" message will be displayed when you press the Turn Off Alarm operation button.

8.10 Duress Options

The terminal will trigger an alarm system after receiving a successful verification from a duress password. Do not using the same method and the same fingerprint during normal working days to avoid triggering the alarm system and disrupting working environment.

8.10.1 Management of Duress Fingerprint

- Press Menu > Options > Access Options > Duress Options > Duress FP >. You can perform four tasks in this operation.

DURESS FP WHAT IS IT FOR

New Enrollment To perform a new fingerprint enrolment for duress purpose

Define Duress FP To define the already enrolled fingerprint for duress purpose

Undefine Duress FP To undefined selected enrolled duress fingerprint from the terminal

Undefine All Duress FP To undefined all enrolled duress fingerprints from the terminal

8.10.2 Help Key

You can configure a Help Key in your terminal to function during duress situations. First, you have to enable the Help Key by: Press Menu > Options > Access Options > Duress Options > Help Key > Y. Then, press and hold the down arrow for 3s followed by the duress fingerprint verification, to trigger alarm.

Summary

* Internal alarm when door is closing properly

* Set alarm for when door is closing within time frame

* DO NOT use same finger or password for normal activity to assign duress finger

ZKSoftware®
The Advanced Biometric Solution

8.10.3 Trigger Methods

The terminals offer 3 types of alarm trigger method.

- Press Menu > Options > Access Options > Duress Options > Choose your method > Y. You can choose one method only.

1. 1:1 Trigger - Triggering alarm using 1:1 method
2. 1:N Trigger - Triggering alarm using 1:N method
3. Password Trigger - Triggering alarm using password method

8.10.4 Alarm Delay

Set the timer to set off the alarm after successful duress finger verification. The time range is from 0 to 254s. The type of output for alarm is NO/NC. Press Menu > Options > Access Options > Duress Options > Alarm Delay > Set your value > OK

8.11 Alarm Count

There is a limit to unsuccessful verification by a user. Predefine the value of unsuccessful verifications so if a user exceeds the allowed times, the alarm will be triggered if your terminal is installed with an alarm system.

- Press Menu > Options > Access Options > Alarm CNT > Define the value > OK

8.12 Group Verification Type

This function offers various verification type(s) for every group that can be set according to time. Description of verification types available in fingerprint terminal is explained in Chapter 4: User.

- Press Menu > Options > Access Options > Group Ver-Type > Select the Group > OK > Select the time > Down arrow and select Verification Type. After finished, press OK

9. RFID CARD FUNCTION

9.1 Understanding the RFID Card

The fingerprint terminals are versatile and it can accept card verifications. This chapter covers the Radio Frequency Identification or better known as RFID system. The terminals accept RFID card with specifications of 64-bit, 125kHz.

9.2 Enrolment of RFID Card

RFID can be enrolled alone, with fingerprint or with password. Each RFID card comes with a unique ID and the terminals will read from the numbers and match it with the card. Enrollment of RFID is easy.

- Press Menu > User Manage > Enroll User/Admin > Reg RFID > OK > Do you want to do new enrollment? > OK > Insert the user ID > OK > Wave the card to the induction area and the machine will display the card number on the LCD along with the User ID > OK > The terminal will display User ID-C meaning that the ID is enrolle with card > OK(Save)

9.3 Verification Using RFID Card Only

In case you want the terminal to read only RFID card, you can configure this selection by selecting RF on Group VerType under Access Options.

Summary

* 3 trigger methods

* Set a trigger alarm delay

* alarm sounds when unseccessful tries has exceeded

* Use RFID card for added security or if user's fingerprint doesn't work

* Enrol RFID card

ZKSoftware®
The Advanced Biometric Solution

9.4 Multi-verification Methods Using RFID

The terminals allow multi-verification where a user is required to use two or more verification methods before he is allowed access to certain areas. Refer to Chapter 4: User, page 19 under Types of Verification Method for more information about different combinations for the terminals and how to configure them. Basically, in order to select different verification methods, make sure that you have registered or enrolled that method in the terminal for the said User ID before any selection is made.

Summary

* User need to verify access with more than one method

9.5 Deleting RFID Card

RFID cards can be used again and again but the information in the card must be deleted first before inserting new information.

* Only administrators can delete

- Press Menu > User Manage > Delete > Input the User ID and wave the card at the induction area > The LCD will ask whether you want to delete the User ID-C > The terminal will ask whether you want to delete User ID > And to delete user. Press OK to all. Once the card has been emptied, it can be used again. Changing Card ID
- Press Menu > User Manage > Enroll User/Admin > Reg RFID > ESC > Change Card ID > Key in Original ID > OK > Wave new card > OK (Save)

10. Autotest

10.1 Who should do the Auto Test?

* Only administrator can do auto tests

Auto Test page is to diagnose or analyze the conditions in the terminal. There are 6 tests available in the Auto Test page and only the administrator is allowed to perform the test.

10.2 Run All Tests At Once

The Auto Test contains 6 tests and to run all of them at once,

- Press Menu > Options > Auto Test > Run All Test > OK > "Pls keep Pwr On" message will be displayed > The terminal will run all tests and when finished the LCD will display the result such as this: All: 31 Bad: 0, to indicate the level of breakdown in the terminal.

10.3 FLASH Test

- Press Menu > Options > Auto Test > FLASH test > OK > "Pls keep Pwr On" message will be displayed > The terminal will run all tests and when finished the LCD will display the result such as this: All: 31 Bad: 0

10.4 LCD Test

- Press Menu > Options > Auto Test > LCD test > OK > The screen will display lines of 'W'. Any missing Ws or jagged W indicates LCD error. Escape to return to the previous page

10.5 Voice Test

- Press Menu > Options > Auto Test > Voice test > OK > The LCD will display for example: "Play Voice 1" and you will hear the message for that. Press OK to listen to the next voice. Any error indictes that something is wrong with the speaker.

10.6 FP Reader

- Press Menu > Options > Auto Test > FP Reader > OK > If your fingerprint sensor is not in good condition, you will see "OK!"

ZKSoftware®
The Advanced Biometric Solution

10.7 Key Test

- Press Menu > Options > Auto Test > Key Test > OK > Press any key and look at the LCD display. If the key matches the description on the LCD, the keypad is in good condition

10.8 RTC Test

Press Menu > Options > Auto Test > RTC test > OK > If the RTC battery is still working, the test will prompt an "OK!"

11. TROUBLESHOOTING

11.1 "Unable to Connect" Appears

When this message appears, it means that the settings for the terminals and the computers are not properly done. Find out which method you are using to connect. Refer to Chapter 3: Connection - Syncing Terminal to further understand the topic.

11.2 "Admin Affirm" Appears

You are not an administrator of this terminal. Only an authorized administrator of the system is allowed to access the Menu. Any attempt of normal user to access the Menu willprompt "Admin Affirm" message on the screen. In case the administrator has resigned from the company, kindly contact your FingerTec authorized reseller to access the terminal.

11.3 Difficult to Read Finger

Five things could be the cause of this:

- Enrolment is not properly done: Enrolment is the most important process to ensure that the terminal captures the best quality of your fingerprints. Refer to chapter 4 for more on how to conduct a good enrolment.
- The location of the terminal is not conducive: The scanner does not work well in brightlighted area. Cover the scanner a little if this is the cause of the difficulty. Shift the location area for a better performance.
- Finger is not properly placed: To get a good reading, make sure that your finger's center points are placed on at the middle of the scanner. Adjust the position of your fingerprint as you see it onscreen.
- The scanner is not cleaned or it is scratched: Check the quality of the scanner. If the scanner is dirty, please clean it with pasting and lifting of a piece of cellophane tape on the scanner. Use a microfiber cloth for a non-coated scanner. If it's scratched, contact your local reseller for a replacement.

Did anything happen to your finger lately? Make sure that the finger is not injured, cut or bruised because it could cause difficulty to read. The algorithm reads the minutiae points of your fingerprint, the more it can read, the better the result.

11.4 The LED is Blinking All The Time

You have nothing to worry about unless the blinking light is red. The green light indicates that terminal is on standby mode. Red blinking light may signal a problem in the terminal. Charge your terminals for a few hours to avoid the red light from blinking. Consult your reseller for technical advice.

11.5 "Duplicate Finger" Appears

FingerTec is an intelligent terminal. It will not accept the same fingerprint twice into its system. If you have registered a finger into a FingerTec device, the system would prompt, "Duplicate Finger" when you try to enroll that finger for another time. Choose a different finger to proceed.

ZKSoftware®
The Advanced Biometric Solution

11.6 RFID Card Doesn't Respond

Summary

Two possibilities for this problem

- ***Have you registered the card to the terminal?*** The card must be registered to the terminal before the terminal could read the information in the card. Refer to chapter 8 User, page 29 for card enrollment.
- ***Have you assigned the user ID to the verification group that supports RFID card?*** Without setting the terminal that you are under a group that supports RFID card, the terminal wouldn't read your card.

11.7 No Sound

A few things could cause this problem:

- The terminal voice mode is silent
- Perhaps someone has turned off the voice in your terminal or reduced its volume to 0%. Refer to Chapter 5 System to under Voice to rectify.
- Speaker is damaged
- Once you have rectified the voice mode and the problem persists, proceed to test the voice. Go to Chapter 12 Auto Test to do the test. If no voice emitted, contact your local reseller for support.

12 System Specification

SPECIFICATION	
Fingerprint Capacity:	3000 templates
Transaction Capacity:	100 000 transactions
Hardware Platform:	ZEM500
Sensor:	ZK Optical sensor
Algorithm Version:	ZK Finger V10.0
Built-in Card Reader:	125 Mhz RFID Reader
Communication:	RS232/485, TCP/IP,USB-host
Wiegand Ports:	Input and Output any bits
Access Control interfaces:	3rd party electric lock, door sensor, exit button, open door alarm.
Access Control functions:	50 time zones, 5 access control groups, 10 unlock combinations

ZKSoftware®
The Advanced Biometric Solution

Appendix A:

F9 Pinout